Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate)

Unit 2: Cyber Security and Incident Management

Sample Assessment Materials

First teaching September 2025

First certification from 2026

Issue 1

About Pearson

We are the world’s leading learning company operating in countries all around the world. We provide content, assessment and digital services to students, educational institutions, employers, governments and other partners globally. We are committed to helping equip students with the skills they need to enhance their employability prospects and to succeed in the changing world of work. We believe that wherever learning flourishes so do people.

References to third party materials made in this document are made in good faith. Pearson does not endorse, approve or accept responsibility for the content of materials, which may be subject to change, or any opinions expressed therein. (Materials may include textbooks, journals, magazines and other publications and websites.)

All information in this specification is correct at time of publication.

VQ000331

All the material in this publication is copyright
© Pearson Education Limited 2024

Contents

Please check the examination details below before entering your candidate information

Candidate surname	Other names

Centre Number

Learner Registration Number

Pearson Level 3 Alternative Academic Qualification BTEC National (Extended Certificate)

Sample assessment material

Time 2 hours 15 minutes

Paper reference **XXXXX/XX**

Information Technology

UNIT 2: Cyber Security and Incident Management

You do not need any other materials.

Total Marks

Instructions

- Use **black** ink or ball-point pen.
- **Fill in the boxes** at the top of this page with your name, centre number and learner registration number.
- Answer **all** questions.
- Answer the questions in the spaces provided – *there may be more space than you need.*

Information

- The total mark for this paper is 90.
- The marks for **each** question are shown in brackets – *use this as a guide as to how much time to spend on each question.*

Advice

- Read each question carefully before you start to answer it.
- Try to answer every question.
- Check your answers if you have time at the end.

Turn over ▶

S80455A

©2023 Pearson Education Ltd.

1/1/1

S 8 0 4 5 5 A 0 1 2 0

Pearson

SECTION A

Read the following scenario carefully. The questions in this section relate to this scenario.

Answer ALL questions. Write your answers in the spaces provided.

Black Country Training and Assessment Associates

Black Country Training and Assessment (BCTAA) offers vocational-based training and assessment services. It specialises in working with small and medium sized businesses which do not wish to set up their own training departments.

BCTAA operates from offices on the 19th floor of a 20-storey building.

Figure 1 shows an incomplete network diagram for the BCTAA system on the 19th floor.

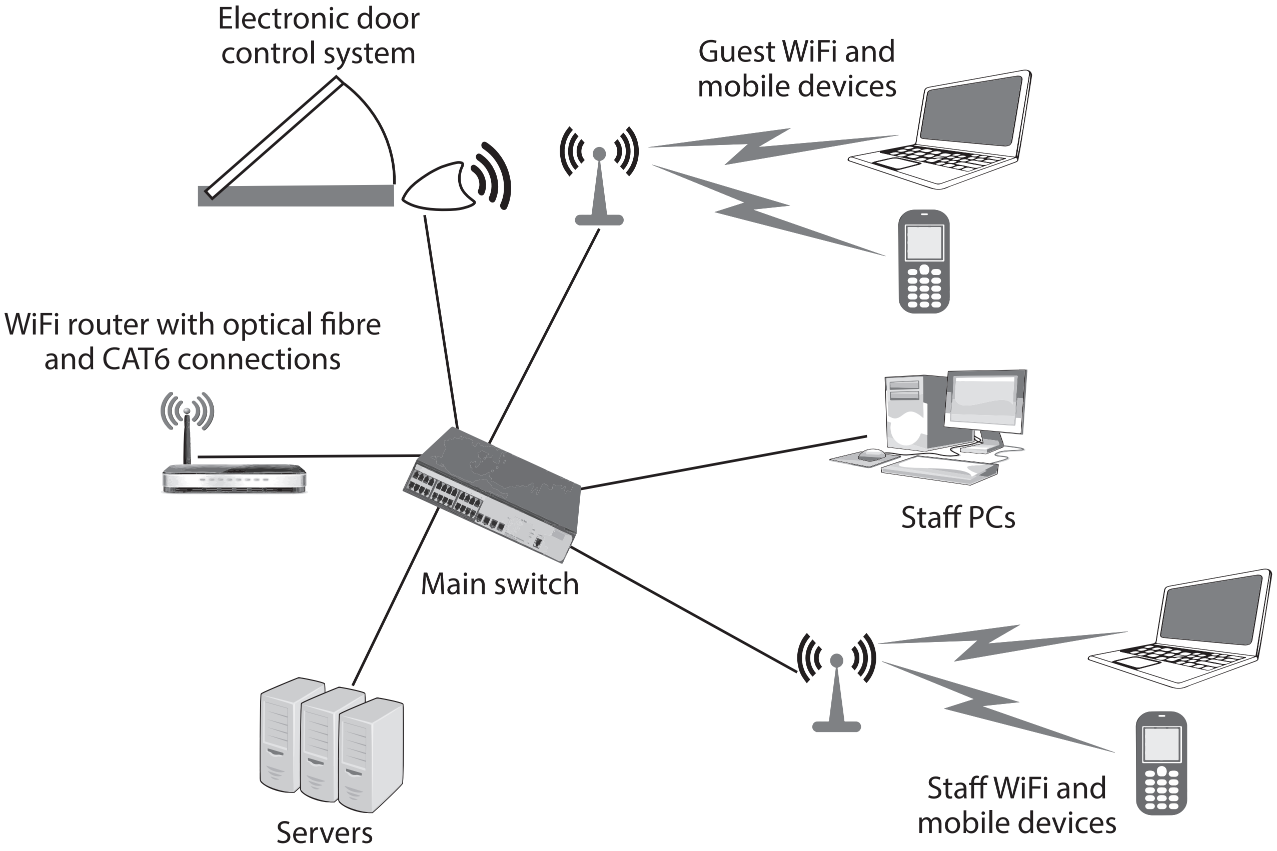

Electronic door control system
Guest WiFi and mobile devices
WiFi router with optical fibre and CAT6 connections
Staff PCs
Main switch
Servers
Staff WiFi and mobile devices

Figure 1

1 (a) BCTAA requires secure internet access.

(i) Complete the network diagram (Figure 1) by adding:

- the device required for a secure internet connection.
- its connection to the network.

The device may be shown as a labelled box.

(2)

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(ii) The network includes wireless access points (WAPs).

Explain **one** vulnerability of a WAP.

(2)

....

....

....

....

(iii) The network environment must be made secure.

Explain **one** way trusted computing can help secure the network against threats.

(2)

....

....

....

....

(b) BCTAAs offices are protected by an electronic door control system.

(i) Intruders could gain entry by tailgating.

State what is meant by tailgating.

(1)

....

....

(ii) Card theft may enable an intruder to gain entry via the system.

Explain **one other** way an intruder could gain entry via the system.

(2)

....

....

....

....

(c) Security threats to the BCTAA network may attack the internet connection, the WAPs and the door control system.

Describe **one other** digital threat to the BCTAA network and an appropriate countermeasure for it.

(4)

(d) The current backup strategy for BCTAA is:

- use RAID 1 – mirrored drives on the servers.
- a daily transfer of working files to a USB stick. There is a set of five, one for each day Monday to Friday, that are reused each week.
- a weekly transfer of all company data to a portable hard drive.
- disk images for all the servers, PCs, and company laptops.

Evaluate the effectiveness of the current backup strategy.

(9)

DO NOT WRITE IN THIS AREA DO NOT WRITE IN THIS AREA DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(Total for Question 1 = 22 marks)

2 (a) The BCTAA network has two WAPs, one for staff and one for guests. Each WAP has a different service set identifier (SSID). The SSIDs can be hidden.

(i) State what an SSID is.

(1)

....

....

(ii) State the purpose of an SSID.

(1)

....

....

(iii) Explain **one** consequence for guests to the BCTAA offices if the SSIDs are hidden.

(2)

....

....

....

....

(b) Guest Wi-Fi is only required for internet access.

The Staff WAP and the Guest WAP connect to a single managed switch. This is a security risk.

Describe how the network should be changed to reduce this risk.

(3)

....

....

....

....

....

....

DO NOT WRITE IN THIS AREA DO NOT WRITE IN THIS AREA DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

(c) BCTAA uses trainers who need to connect to BCTAA over the internet. They use a virtual private network (VPN), run from a BCTAA server.

(i) Describe how **this** VPN functions.

(3)

....

....

....

....

....

....

(ii) State **two** drawbacks for BCTAA in using the VPN to communicate with their trainers.

(2)

1 ....

....

2 ....

....

(d) BCTAA staff log into the network with a username and password, but when they need to access highly confidential information, they must also plug in a USB security key for multi-factor authentication (MFA).

Explain how a USB security key works.

(2)

....

....

....

....

(e) BCTAA is considering the use of Media Access Control (MAC) address filtering to protect the Staff and Guest Wi-Fi.

Evaluate the use of MAC address filtering on the BCTAA Wi-Fi.

(9)

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(Total for Question 2 = 23 marks)

3 (a) BCTAA has several servers, including a Dynamic Host Configuration Protocol (DHCP) server.

When the DHCP server is configured, the administrator must enter configuration information, including the default gateway address.

State **two other** pieces of configuration information that must be entered.

(2)

....

....

....

....

(b) DHCP is inherently insecure, as it does not have any built-in security measures. This leaves DHCP open to attack.

Describe **one** method of attacking the BCTAA network by exploiting DHCP.

(3)

....

....

....

....

....

....

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

(c) BCTAA hosts its website on its own web server.

It has been attacked by Structured Query Language (SQL) injection and by Distributed Denial of Service Attacks (DDoS)

(i) Describe how an SQL injection attack works

(3)

....

....

....

....

....

....

(ii) Explain **one** method of preventing SQL injection.

(2)

....

....

....

....

(d) The BCTAA servers have been subject to denial-of-service attacks over the internet, both DoS and DDoS.

(i) Describe the difference between DoS and DDoS attacks

(2)

....

....

....

....

(ii) Explain how such a denial of service (DoS) attack is carried out.

(2)

....

....

....

....

(e) BCTAA has WAPs for staff and guests. Each WAP can be configured to use Wi-Fi Protected Access 2 (WPA2) or WPA3.

Evaluate the use of WPA2 and WPA3 on the BCTAA WAPs.

(9)

....

....

....

....

....

....

....

....

....

....

....

DO NOT WRITE IN THIS AREA DO NOT WRITE IN THIS AREA DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(Total for Question 3 = 23 marks)

4 BCTAA has a staff Password Policy. It has sections on:

- length and complexity
- password sharing
- password uniqueness

(a) Give **two other** sections that a password policy should contain.

(2)

....

....

....

....

(b) BCTAA encourages staff to use a password manager.

(i) Explain **one** advantage of using a password manager

(2)

....

....

....

....

(ii) Explain **one** disadvantage of using a password manager

(2)

....

....

....

....

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

(c) A staff member thinks that their password manager may have been compromised.

The IT Manager takes a physical image of the tablet's entire drive, rather than a targeted image of the files related to the password manager.

(i) Explain why the physical image is made instead of the targeted image.

(2)

....

....

....

....

(ii) Describe the process for creating the image of the tablet's drive.

(3)

....

....

....

....

....

....

(d) The physical image contains copies of the tablet's log files.

Explain which log file is likely to contain evidence about the possible compromise of the password manager.

(2)

....

....

....

....

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

(e) A plan of BCTAAs offices on the 19th floor is shown in Figure 2.

The lifts, stairwells, WCs and associated areas are open to the public. The remaining area is a single open space which can be partitioned to create rooms or workspaces.

Threats already identified include the use of a single switch for WAPs, no MAC filtering, the backup process and the use of a password manager.

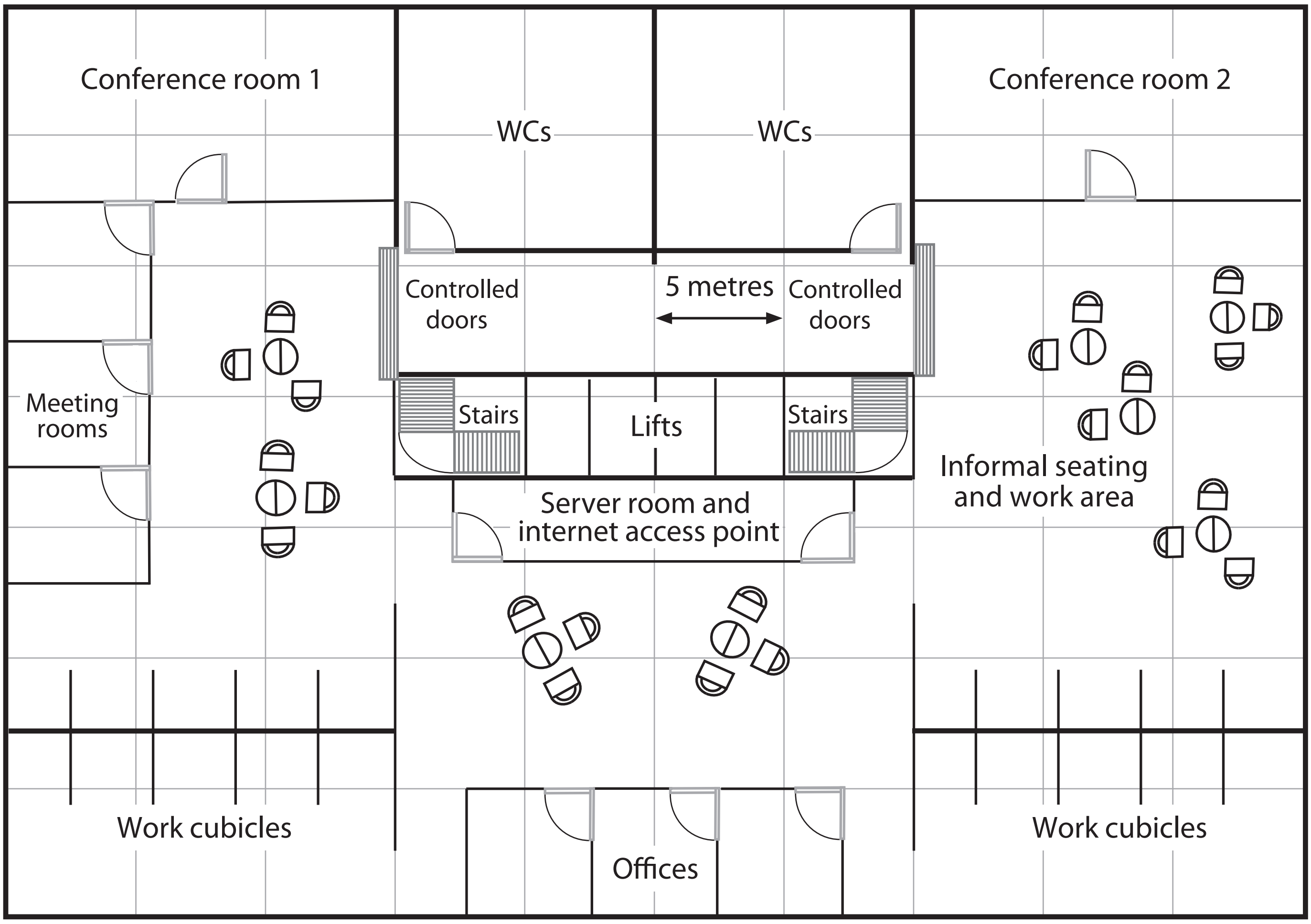


Figure 2

Evaluate the management of security threats to the BCTAA offices in this scenario, that have not been previously identified.

(9)

....

....

....

....

....

....

DO NOT WRITE IN THIS AREA DO NOT WRITE IN THIS AREA DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

(Total for Question 4 = 22 marks)

TOTAL FOR SECTION A = 90 MARKS

General marking guidance

- All students must receive the same treatment. Examiners must mark the first student in exactly the same way as they mark the last.
- Mark schemes should be applied positively. Students must be rewarded for what they have shown they can do rather than be penalised for omissions.
- Examiners should mark according to the mark scheme, not according to their perception of where the grade boundaries may lie.
- All marks on the mark scheme should be used appropriately.
- All the marks on the mark scheme are designed to be awarded. Examiners should always award full marks if deserved. Examiners should also be prepared to award zero marks if the student's response is not rewardable according to the mark scheme.
- Where judgement is required, a mark scheme will provide the principles by which marks will be awarded.
- When examiners are in doubt regarding the application of the mark scheme to a student's response, a senior examiner should be consulted.
- Crossed out work should be marked unless the student has replaced it with an alternative response.
- Accept incorrect/phonetic spelling (as long as the term is recognisable) unless instructed otherwise.

Edexcel and BTEC Qualifications

Edexcel and BTEC qualifications come from Pearson, the world's leading learning company. We provide a wide range of qualifications including academic, vocational, occupational and specific programmes for employers. For further information visit our qualifications website at http://qualifications.pearson.com/en/home.html for our BTEC qualifications.

Alternatively, you can get in touch with us using the details on our contact us page at http://qualifications.pearson.com/en/contact-us.html

If you have any subject specific questions about this specification that require the help of a subject specialist, you can speak directly to the subject team at Pearson.
Their contact details can be found on this link:
http://qualifications.pearson.com/en/support/support-for-you/teachers.html

You can also use our online Ask the Expert service at https://www.edexcelonline.com
You will need an Edexcel Online username and password to access this service.

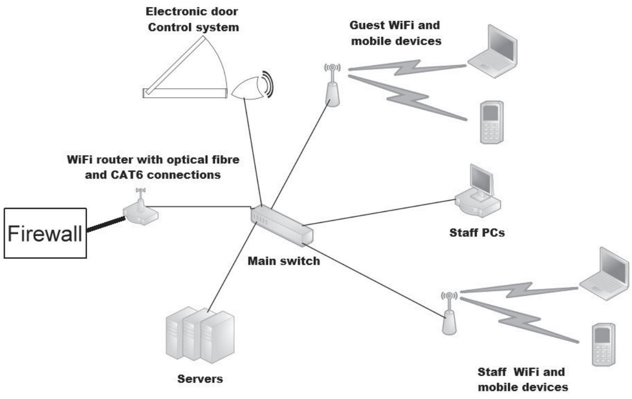
Pearson: helping people progress, everywhere

Our aim is to help everyone progress in their lives through education. We believe in every kind of learning, for all kinds of people, wherever they are in the world. We've been involved in education for over 150 years, and by working across 70 countries, in 100 languages, we have built an international reputation for our commitment to high standards and raising achievement through innovation in education. Find out more about how we can help you and your students at: www.pearson.com/uk.

Draft

December 2023
Publications Code VQ000311

All the material in this publication is copyright
© Pearson Education Ltd 2023

Question Number	Answer	Mark
1 ai	Award **one** mark for Firewall as a device/box/shape. Award **one** mark for the Firewall device/box/shape connected to the router by a solid line.  Electronic door Control system Guest WiFi and mobile devices WiFi router with optical fibre and CAT6 connections Firewall Main switch Staff PCs Servers Staff WiFi and mobile devices	2

Question Number	Answer	Mark
1 aii	Award **one** mark for a reason, and **one** mark for an appropriate linked expansion, up to a maximum of **two** marks. • WiFi can be accessed from public areas (1) because radio signals pass outside the offices/go through the walls (1) • WiFi is available to guests (1) they may bring in malware (on their devices) (1) Accept any other appropriate/alternative response.	2

Question Number	Answer	Mark
1 aiii	Award **one** mark for a way, and **one** mark for an appropriate linked justification/expansion, up to a maximum of **two** marks. • reduces the risk of cyber-attacks (1) provides another layer/two-step verification/encryption key/protection/increased security (1) • prevent disruption of network functions (1) defends against external threats/malware to minimise network disruption (1) Accept any other appropriate/alternative response.	2

Question Number	Answer	Mark
1 bi	Award **one** mark for the following: • following an (authorised) person through the door before it shuts (1) Accept any other appropriate/alternative response.	1

Question Number	Answer	Mark
1 bii	Award **one** mark for a process, and **one** mark for an appropriate linked expansion, up to a maximum of **two** marks. • card cloning/skimming where a card is 'read' (1) and copied onto a new card/device (1) • signal interception/range extension where the card is read by one device (1) and the signal transmitted to another device/the door reader (to open the door) (1) Accept any other appropriate/alternative response. Do not accept any form of theft/borrowing of the card.	2

Question Number	Answer	Mark
1 c	Award **one** mark for each appropriate point in a linked description up to a maximum of **four** marks. • identification of an electronic threat (1) • identification of a suitable countermeasure (1) • description of how the countermeasure is enabled (1) • description of how it reduces the threat (1) Examples: • malware on USB (1) • use a PCs BIOS settings (1) • disable USB input (1) • USB sticks cannot be used to insert a virus (1) or • incorrect access level settings (1) • use admin settings/group policy/security settings on the server (1) • set the correct group/level/policy (1) • user access is restricted/limited to specific files/areas (1) Points in a process must be the correct position to gain marks. Accept any other appropriate/alternative response. Do not accept: • physical threats • threats from the internet • threats to the WAP • threats to the door controls	4

Question Number	Answer	Mark
1 d	Responses will be credited according to the student's demonstration of knowledge and understanding of the material, using the indicative content and level descriptors below. The indicative content that follows is not prescriptive. Responses may cover some or all indicative content, but students should be rewarded for other relevant responses. Students will evaluate the effectiveness of the backup strategy. Mirrored drives: • not for backup • used to stop data loss when a drive fails • corruption/virus etc on one would affect both USB for daily backup: • possible but slow to write, especially if lots of data • possibility of losing/mislaying • easily damaged/ accidentally corrupted • relies on personal security when travelling/at home Portable drive for weekly backup: • similar to USB problems • all eggs in one basket Disk images: • not strictly backup but possible solution for disaster recovery/reset for new user, especially for laptops and PCs • server disks need to be kept secure and have a copy not at BCTAA in case of fire etc.	9

Mark scheme (award up to 9 marks) refer to the Levels-Based Mark Scheme Guidance for how to apply levels-based mark schemes*.		
Level	Mark	Descriptor
Level 0	0	No rewardable material
Level 1	1-3	• Demonstrates basic application of knowledge and understanding that is partially relevant to the context of the question and may consider only one side of the context (AO2) • Demonstrates a basic analysis of the situation by superficially breaking down the different aspects into their component parts. (AO3a) • Demonstrates a basic evaluation which partially considers different factors/events and competing points, leading to a conclusion which is superficial or unsupported. (AO3b)
Level 2	4-6	• Demonstrates good application of knowledge and understanding that is relevant to the context of the question and considers both sides of the context. (AO2) • Demonstrates a good analysis of the situation by breaking down the different aspects into their component parts. (AO3a) • Demonstrates a good evaluation which considers different factors/events and competing points, leading to a conclusion which is partially supported. (AO3b)
Level 3	7-9	• Demonstrates comprehensive application of knowledge and understanding that is consistently relevant to the context of the question and considers both sides of the context in a balanced way. (AO2) • Demonstrates a thorough analysis of the situation by comprehensively breaking down the different aspects into their component parts. (AO3a) • Demonstrates a thorough evaluation which comprehensively considers different factors/events and competing points, leading to a conclusion which is well supported. (AO3b)

Question Number	Answer	Mark
2 ai	Award **one** mark for the following: • the name broadcast (by a Wi-Fi network) (1) Accept any other appropriate/alternative response.	1

Question Number	Answer	Mark
2 aii	Award **one** mark for the following: • to allow the identification/log on to the correct network (1) Accept any other appropriate/alternative response.	1

Question Number	Answer	Mark
2 aiii	Award **one** mark for a reason, and **one** mark for an appropriate linked expansion, up to a maximum of **two** marks. • guests' device may try to disconnect/connect to other network (1) as OS prefers SSID networks over non-SSID (1) • guests will have to ask (staff) for Wi-Fi details (1) as they cannot see the network on their (mobile) devices (1) • guests may need to set-up auto-reconnect (for future visits) (1) device then pings/uses extra power when away from the network (1) • guests will need to ask for/enter network details on each visit (1) this is time consuming/poor customer relations (1) Accept any other appropriate/alternative response. Do not accept answers relating to problems/inconvenience for staff.	2

Question Number	Answer	Mark
2 b	Award **one** mark for each appropriate point in a linked description up to a maximum of **three** marks. • use a second switch (1) • to divide/segment the network (1) • so that guest traffic ○ only connects to the router/internet access point (1) ○ does not use/access the rest of the network (1) Points in a process must be the correct position to gain marks. Accept any other appropriate/alternative response.	3

Question Number	Answer	Mark
2 ci	Award **one** mark for each appropriate point in a linked description up to a maximum of **three** marks. • establishes a protected/private/direct connection (1) • encrypts the data (1) • reduces risk of interception/man-in-the-middle attack (1) • doesn’t route through/reduces routing through third party servers (1) Accept any other appropriate/alternative response. Do not accept answers relating to VPN run by a third party.	3

Question Number	Answer	Mark
2 cii	Award **one** mark for each point up to a maximum of **two** marks. • cost of running the server/VPN (1) • VPN is (usually) slower than normal internet traffic (1) • VPN uses more data than normal internet traffic (1) • VPN may be illegal if trainers are in some foreign countries (1)	2

Question Number	Answer	Mark
2 d	Award **one** mark for an identification, and **one** mark for an appropriate linked expansion, up to a maximum of **two** marks. • USB key/chip contains code/protocol(1) that can be read/checked by the server/network/system to verify identity (1) Only acceptable response.	2

Question Number	Answer	Mark
2 e	Responses will be credited according to the student's demonstration of knowledge and understanding of the material, using the indicative content and level descriptors below. The indicative content that follows is not prescriptive. Responses may cover some or all indicative content, but students should be rewarded for other relevant responses. Students will evaluate the use of MAC address filtering on the BCTAA Wi-Fi Staff: • would need to set-up list once • only need to modify for new devices • helps prevent intrusion by unlisted devices Guests: • would need to set-up new entries for each new guest/guest device • takes more time and resources • WAPs often have limited size MAC list which could cause problems if there are many guests/devices • inconvenient for new guests – would ned to know/find their MAC address • extra security is not needed on Guest Wi-Fi General: • helps with security but cost-benefit is different for Staff/Guest network • MAC addresses can be spoofed so only medium security	9

Mark scheme (award up to 9 marks) refer to the Levels-Based Mark Scheme Guidance for how to apply levels-based mark schemes*.		
Level	Mark	Descriptor
Level 0	0	No rewardable material
Level 1	1-3	• Demonstrates basic application of knowledge and understanding that is partially relevant to the context of the question and may consider only one side of the context (AO2) • Demonstrates a basic analysis of the situation by superficially breaking down the different aspects into their component parts. (AO3a) • Demonstrates a basic evaluation which partially considers different factors/events and competing points, leading to a conclusion which is superficial or unsupported. (AO3b)
Level 2	4-6	• Demonstrates good application of knowledge and understanding that is relevant to the context of the question and considers both sides of the context. (AO2) • Demonstrates a good analysis of the situation by breaking down the different aspects into their component parts. (AO3a) • Demonstrates a good evaluation which considers different factors/events and competing points, leading to a conclusion which is partially supported. (AO3b)
Level 3	7-9	• Demonstrates comprehensive application of knowledge and understanding that is consistently relevant to the context of the question and considers both sides of the context in a balanced way. (AO2) • Demonstrates a thorough analysis of the situation by comprehensively breaking down the different aspects into their component parts. (AO3a) • Demonstrates a thorough evaluation which comprehensively considers different factors/events and competing points, leading to a conclusion which is well supported. (AO3b)

Question Number	**Answer**	**Mark**
3 a	Award **one** mark for any of the following, up to a maximum of **two** marks. • range of (available) IP addresses (1) • fixed IP addresses (1) • lease length (1) Accept any other appropriate/alternative response.	2

Question Number	Answer	Mark
3 b	Award **one** mark for each appropriate point in a linked description up to a maximum of **three** marks. • spoofing/using a false/rogue DHCP server (1) • to supply clients/devices with fake/wrong configuration information (1) • to enable man-in-the-middle attack (1) / to disrupt/prevent network traffic (1) or • spoofing/using a false/rogue DHCP client (1) • to make repeated (DHCP) requests (1) • to use up the available addresses (1) / to disrupt/prevent network traffic (1) Points in a process must be the correct position to gain marks. Accept any other appropriate/alternative response.	3

Question Number	Answer	Mark
3 ci	Award **one** mark for each appropriate point in a linked description up to a maximum of **three** marks. • query input to (online) database (1) • (query) contains SQL statement/instruction written/designed to cause unauthorised action (1) • to reveal/attack/steal/disrupt/delete data (1) Points in a process must be the correct position to gain marks. Accept any other appropriate/alternative response.	3

Question Number	Answer	Mark
3 cii	Award **one** mark for an identification, and **one** mark for an appropriate linked expansion, up to a maximum of **two** marks. • only allow pre-made queries/selection from query list (1) to prevent rogue SQL (statements) from being run/executed (1) or • use a script or web application firewall (1) to sanitise/check/test SQL statements before they run (1) Accept any other appropriate/alternative response.	2

Question Number	Answer	Mark
3 di	Award **one** mark for each appropriate point in a linked description up to a maximum of **two** marks. • DoS attack comes from single device/source/system/IP address (1) • DDoS involves multiple devices/sources/systems/IP addresses (1) Only acceptable responses.	2

Question Number	Answer	Mark
3 dii	Award **one** mark for an identification, and one mark for an appropriate linked expansion, up to a maximum of **two** marks. • server/gateway receives/is sent large number of pings/packets/service requests (1) so that the server/system is overwhelmed/cannot service all the requests (1) or • server/gateway receives/is sent large number of pings/packets/service requests (1) so that the server/system slows/stops/crashes/is unable to perform normal functions (1) Accept any other appropriate/alternative response.	2

Question Number	Answer	Mark
3 e	Responses will be credited according to the student's demonstration of knowledge and understanding of the material, using the indicative content and level descriptors below. The indicative content that follows is not prescriptive. Responses may cover some or all indicative content, but students should be rewarded for other relevant responses. Students will evaluate the use of WPA2 and WPA3 on the BCTAA WAPs Handshake: • WPA2 uses the Pre-Shared Key (PSK) exchange WPA3 uses Simultaneous Authentication of Equals (SAE) Encryption/data transfer: • WPA3 has faster encryption rates but requires more processing power • Both use AES but WPA3 uses/can use (depending on version) longer encryption strings (up to AES-256) • WPA3 more resistant to offline/dictionary attack General: • WPA3 is relatively new (2018) • Older devices/OSs do not support WPA3 • WPA3 is more secure • BCTAA can ensure staff devices are compatible with WPA3 • Guest devices may not be compatible with WPA3 • Guest devices capable of using WPA3 will have legacy compatibility with WPA2	9

Mark scheme (award up to 9 marks) refer to the Levels-Based Mark Scheme Guidance for how to apply levels-based mark schemes*.		
Level	Mark	Descriptor
Level 0	0	No rewardable material
Level 1	1-3	• Demonstrates basic application of knowledge and understanding that is partially relevant to the context of the question and may consider only one side of the context (AO2) • Demonstrates a basic analysis of the situation by superficially breaking down the different aspects into their component parts. (AO3a) • Demonstrates a basic evaluation which partially considers different factors/events and competing points, leading to a conclusion which is superficial or unsupported. (AO3b)
Level 2	4-6	• Demonstrates good application of knowledge and understanding that is relevant to the context of the question and considers both sides of the context. (AO2) • Demonstrates a good analysis of the situation by breaking down the different aspects into their component parts. (AO3a) • Demonstrates a good evaluation which considers different factors/events and competing points, leading to a conclusion which is partially supported. (AO3b)
Level 3	7-9	• Demonstrates comprehensive application of knowledge and understanding that is consistently relevant to the context of the question and considers both sides of the context in a balanced way. (AO2) • Demonstrates a thorough analysis of the situation by comprehensively breaking down the different aspects into their component parts. (AO3a) • Demonstrates a thorough evaluation which comprehensively considers different factors/events and competing points, leading to a conclusion which is well supported. (AO3b)

Question Number	Answer	Mark
4 a	Award **one** mark for any of the following up to a maximum of **two** marks: • password reuse/recycling (1) • password changing/expiry (1) • failed logins – threshold/number allowed (1) • failed logins – recovery procedure (1) Accept any other appropriate/alternative response. Do not accept: • password length and complexity • password sharing • password uniqueness.	2

Question Number	Answer	Mark
4 bi	Award **one** mark for an identification, and **one** mark for an appropriate linked expansion, up to a maximum of **two** marks. • password manager generates a (complex) password (1) to ensure higher security passwords are used (1) • single point of password storage (1) so only the master password needs to be memorised (1) • password manager is cloud-based (1) so it can be accessed on multiple devices (1) Accept any other appropriate/alternative response.	2

Question Number	Answer	Mark
4 bii	Award **one** mark for an identification, and one mark for an appropriate linked expansion, up to a maximum of **two** marks. • single point of failure/place to attack (1) so can lose all passwords at once (1) • some expertise needed to set it up/maintain (1) configuration errors can leave passwords vulnerable (1) • may store data in the cloud (1) relying on third party security (1) Accept any other appropriate/alternative response.	2

Question Number	Answer	Mark
4 ci	Award **one** mark for an identification, and **one** mark for an appropriate linked expansion, up to a maximum of **two** marks. • physical image contains deleted files/data fragments/part files (1) so previous/deleted copies/versions of the password manager/files can be seen/examined (1) • targeted image only has latest/entire/current version/file (1) so cannot see deleted/altered versions (1) Accept any other appropriate/alternative response.	2

Question Number	Answer	Mark
4 cii	Award **one** mark for each appropriate point in a linked description up to a maximum of **three** marks. • connect tablet to device/USB with forensic/copying/imaging/scanning software/program (1) • block/stop any write operations on the tablet (1) • take a bit-by-bit/exact/mirror copy of the drive (1) • log time-date/document the action (1) Points in a process must be the correct position to gain marks. Accept any other appropriate/alternative response.	3

Question Number	Answer	Mark
4 d	Award **one** mark for an identification, and **one** mark for an appropriate linked expansion, up to a maximum of **two** marks. • application/app log (1) because it shows when the password manager was run/started/stopped (1) • event log (1) because it shows user/system activities (1) Accept any other appropriate/alternative response	2

Question Number	Answer	Mark
4 e	Responses will be credited according to the student's demonstration of knowledge and understanding of the material, using the indicative content and level descriptors below. The indicative content that follows is not prescriptive. Responses may cover some or all indicative content, but students should be rewarded for other relevant responses. Students will evaluate the management of security threats to the BCTAA offices. Threats should be within the offices/floor. External threats should not be considered. Threats/vulnerabilities mentioned in the paper: • WAPs • door controls • passwords/login • DHCP • poor backup procedures Threats/vulnerabilities implied by the scenario/figures: • eavesdropping, physical and electronic, from public areas • eavesdropping from floors above/below • clients/visitors overhearing sensitive conversations/seeing sensitive material on screen • clients/visitors could get access to BCTAA systems/ unattended devices • clients/visitors could exploit USB/Bluetooth for malicious uses Security of threats: Novel observations of the security such as the ones in italics, should gain credit. Rehashing of items/answers mentioned in the paper should not be credited: • *door controls – no card protection/screening* • *use of multi-factor authentication* • *no port security on switch* • *limit number of MAC addresses allowed per port* • *no sound insulation* • *use of protected rooms for sensitive discussions* • *WAP range* • *radio/WiFi shielding* • *lock unattended devices/screens* • *guests not being accompanied* • *security of Bluetooth/USB/other means of access by blocking/disabling/encryption*	9

<table>
<tr><th colspan="3"><b>Mark scheme (award up to 9 marks)</b> refer to the Levels-Based Mark Scheme Guidance for how to apply levels-based mark schemes*.</th></tr>
<tr><td>Level</td><td>Mark</td><td>Descriptor</td></tr>
<tr><td>Level 0</td><td>0</td><td>No rewardable material</td></tr>
<tr><td>Level 1</td><td>1-3</td><td>• Demonstrates basic application of knowledge and understanding that is partially relevant to the context of the question and may consider only one side of the context (AO2)
• Demonstrates a basic analysis of the situation by superficially breaking down the different aspects into their component parts. (AO3a)
• Demonstrates a basic evaluation which partially considers different factors/events and competing points, leading to a conclusion which is superficial or unsupported. (AO3b)</td></tr>
<tr><td>Level 2</td><td>4-6</td><td>• Demonstrates good application of knowledge and understanding that is relevant to the context of the question and considers both sides of the context. (AO2)
• Demonstrates a good analysis of the situation by breaking down the different aspects into their component parts. (AO3a)
• Demonstrates a good evaluation which considers different factors/events and competing points, leading to a conclusion which is partially supported. (AO3b)</td></tr>
<tr><td>Level 3</td><td>7-9</td><td>• Demonstrates comprehensive application of knowledge and understanding that is consistently relevant to the context of the question and considers both sides of the context in a balanced way. (AO2)
• Demonstrates a thorough analysis of the situation by comprehensively breaking down the different aspects into their component parts. (AO3a)
• Demonstrates a thorough evaluation which comprehensively considers different factors/events and competing points, leading to a conclusion which is well supported. (AO3b)</td></tr>
</table>

July 2024

For information about Pearson Qualifications, including Pearson Edexcel and BTEC qualifications visit qualifications.pearson.com

Edexcel and BTEC are registered trademarks of Pearson Education Limited

Pearson Education Limited. Registered in England and Wales No. 872828
Registered Office: 80 Strand, London WC2R 0RL.

VAT Reg No GB 278 537121